APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/701,157	11/22/2000	George Friedman	1206-00	7408

35811   7590   09/08/2006

IP GROUP OF DLA PIPER RUDNICK GRAY CARY US LLP
1650 MARKET ST
SUITE 4900
PHILADELPHIA, PA   19103

EXAMINER
CALLAHAN, PAUL E

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 09/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/701,157	FRIEDMAN ET AL.
	Examiner	Art Unit
	Paul Callahan	2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>15 June 2006</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-149</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1,2,4,5,66-68,95-97,129,130 and 148</u> is/are rejected.

7)☐ Claim(s) <u>3,6-65,69-94,98-128,131-147 and 149</u> is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1-149 are pending in this application and have been examined.

Response to Arguments

2.   Applicant's arguments filed 6-15-06 have been fully considered but they are not

fully persuasive.

        a.)   The applicant argues in traverse of the rejection of claims 1-5 and 8 under

35 USC 102(e) as anticipated by Saito, US 5,848,158 (henceforth Saito) by asserting

that Saito fails to teach the feature of the claimed invention as set forth in claim 1 of

bundling data and one or more permissions for use of the data together for delivery to a

user. Yet a review of Saito shows that such is indeed taught, for example at col. 5 lines

38-45, and col. 6 line 53 through col. 7 line 5 where a plaintext copyright label is sent

along with encrypted data to a user. The label is necessary for the user to acquire the

key needed to decrypt the data and hence does read on a reasonably broad

interpretation of permission data since the copyright label gives the user permission to

seek a decryption key.

        The applicant asserts that Saito fails to teach use of a "vault" for storage of the

encrypted data stating: "*Furthermore, Saito fails to disclose storing the data in a vault.*

As noted above, a vault refers to allocated space on a receiver's hard drive for

protecting and hiding vault contents". Yet such limitations are not found in the claims

and the applicant is therefore arguing based on features absent from the claims. Saito

does teach encrypting the data with a "crypt key" prior to storage. This does read on a

reasonably broad interpretation of vault since in many instances in the prior art a vault

refers to strong encryption rather than a physical location. Therefore, in response to

applicant's argument that the references fail to show certain features of applicant's

invention, it is noted that the features upon which applicant relies are not recited in the

rejected claim(s). Although the claims are interpreted in light of the specification,

limitations from the specification are not read into the claims. See *In re Van Geuns*, 988

F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

The applicant asserts that Saito fails to teach "verifying the receiver". Yet the step

of Saito wherein a user sends a plaintext copyright label does read on a reasonably

broad interpretation of verifying a user since this step does verify that a user possesses

the copyright label and hence is the original receiver of the data.

The applicant asserts that Saito fails to teach "opening the package" as recited in

claim 2. Yet the cited section of Saito, col. 5 lines 24-45 does teach accessing the

package, and use of the copyright label to obtain the necessary key to decrypt the rest

of the package. This does read on a reasonably broad interpretation of opening the

package and verifying the receiver.

The applicant argues that Saito fails to teach providing "internal security" as

recited by claim 5. The Applicant states: *"Internal security, as used in Claim 5, refers to*

additional security features contained within the vault for use in further preventing

unauthorized access to protected data stored in the vault, as opposed to providing

general security internal to a receiver. (see page 5, lines 17-26 of the specification)." In

response to applicant's argument that the references fail to show certain features of

applicant's invention, it is noted that the features upon which applicant relies are not

recited in the rejected claim(s). Although the claims are interpreted in light of the

specification, limitations from the specification are not read into the claims. See *In re*

Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

        b.)   The Applicant argues in traverse of the rejections of the claims 95-97, 129,

130, and 148 under 35 USC 102(3) as anticipated by Schneck et al., US 5,933,498

(henceforth Schneck).

        The Applicant asserts that Schneck fails to teach the use of a vault to

store the data as set forth in claims 95 and 129. The Applicant states: *"Unlike other hard*

drive spaces, however, a vault is unique in that its existence, and the existence of any

data stored therein, is invisible to a user of the receiver. (see page 4, line 21 to page 6,

line 12 of the specification)." In response to applicant's argument that the references fail

to show certain features of applicant's invention, it is noted that the features upon which

applicant relies are not recited in the rejected claim(s). Although the claims are

interpreted in light of the specification, limitations from the specification are not read into

the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

        The applicant argues that the cited portion of Schneck: fig., 1, col. 15 line 50

through col. 16 line 20, cannot teach a "vault". Yet the cited sections teach a secure

physical memory location with both physical and logical security measures that prevent

unauthorized access. This does indeed read on a reasonably broad interpretation of a "vault" for storing data.

The applicant argues that the vault of Schneck cannot read on the limitations recited in claim 96 of "internal security". The Applicant states: "*Claim 96 depends from Claim 95, and recites providing internal security. Internal security, as used in Claim 96, refers to additional security features contained within the vault for use in further preventing unauthorized access to protected data stored in the vault, as opposed to providing general security internal to a receiver. (see page 5, lines 17-26 of the specification).*" In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). In addition, the security features of the secure memory location, both physical and logical, are indeed "internal" security features under a reasonably broad interpretation of that term.

The Applicant argues that Schneck fails to teach bundling data and at least one permissions together in one computer system, and storing the package in a vault in another computer system. The applicant states that Schneck does not teach a vault at the second computer. The Examiner again maintains that Schneck does indeed teach such as per the discussion supra.

c.)   The applicant argues in traverse of the rejection of claims 66–68 under 35
U.S.C. 103(a) as being unpatentable over Saito and Schneck US 5,933,498.

The applicant reiterates the argument that neither Saito nor Schneck teach a
vault for secure storage as recited by claim 66. The Examiner again maintains that such
is indeed taught by Saito and Schneck as discussed supra.

The applicant asserts that the combination of Saito and Schneck fail to teach a
package of data bundled together with one or more permissions. The Examiner
maintains again that such is indeed taught by Saito and Schneck as discussed supra.

The Applicant argues in traverse of the taking of Official Notice in the previous
Office Action, that setting a password for access to a computer executable file is a step
that is old and well known in the art. In response, the Applicant's attention is called now
to Schull, US 7,092,908, in the abstract, fig. 1 item 45, and fig. 2 item 240 where
password access to an executable file is explicitly taught.

The applicant's arguments in traverse of the rejections of claim 3, 6, 8, and 40-65
are persuasive and the rejections of those claims are withdrawn.

Claim Rejections - 35 USC § 102

3.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that
form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

4.   The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act

of 1999 (AIPA) and the Intellectual Property and High Technology Technical

Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting

directly or indirectly from an international application filed before November 29, 2000.

Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior

to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

5.   Claims 1, 2, 4, and 5, are rejected under 35 U.S.C. 102(e) as being anticipated

by Saito et al. US 5,848,158.

As for claim 1, Saito teaches a method for maintaining data security comprising:

creating a package comprising data and one or more permissions for regulating use of

the data; and providing a receiver for processing the package and storing the data in a

vault. (col. 2 lines 60-67).

As for claim 2, Saito teaches a method according to claim 1, wherein the step of

processing the package further comprises opening the package and verifying the

receiver for processing of the package (col. 5 lines 24-45).

As for claim 4, Saito teaches a method according to claim 1 further comprising

detecting violations of said one or more permissions (col. 2 lines 56-59).

As for claim 5, Saito teaches a method according to claim 4 wherein the step of

providing a receiver further comprises providing internal security (col. 4 lines 50-59).

6.   Claims 95-97, 129, 130, and 148 are rejected under 35 U.S.C. 102(e) as being

anticipated by Schneck, US 5,933,498

As for claims 95 and 129, Schneck teaches a system and a computer program

product embodied in a memory medium for directing for maintaining data security

comprising: a receiver for processing a package comprising data and one or more

permissions for regulating use of the data; and a vault for storing the data (fig. 1, col. 15

line 50 through col. 16 line 20).

As for claim 96, Schneck teaches a system according to claim 95 further

comprising internal security for protecting the data stored in the vault (col. 15 line 50

through col. 16 line 20).

As for claims 97 and 130, Schneck teaches a system and a computer program

product for directing the system according to claim 96, wherein the internal security

further detects violation of said one or more permissions (col. 18 lines 10-60, col. 15

lines 20-25).

As for claim 148, Schneck teaches a system for maintaining security during

transmission of data between at least two computers comprising: a first computer

having a system for creating a package comprising data and one or more permissions

selected from a list of available permissions for regulating use of the data; and a second

computer having a system for receiving the package from the first computer, opening

the package upon verification and storing the data in a vault (figs. 1-3, col. 15 line 50

through col. 16 line 20, col. 18 lines 10-60).

Claim Rejections - 35 USC § 103

7.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

8.   Claims 66–68 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Saito and Schneck US 5,933,498.

As for claim 66, Saito teaches all of the limitations of claim 1 upon which claim 66

depends, but does not teach: receiving a file of data for packaging; receiving a

permissions database having one or more permissions associated with the file of data,

the one or more permissions governing a client's use of the file; generating a package

global unique identifier; generating a package of data comprising the file, the one or

more permissions and the global unique identifier; encrypting the package; and

generating a computer executable file comprising the encrypted package. However

Schneck does teach these features (figs. 1-3, col. 13 lines 17-27, col. 29 lines 27-57).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the

invention to incorporate the features of Schneck into the system of Saito. Motive to

make this combination is found for example, at col. 2 lines 18-27 where the desirability

of copyright control systems allowing distributors control of end user use of copyrighted

materials is discussed.

As for claim 67, Saito does not teach the method of claim 66 wherein the one or

more permissions are selected from the group consisting of: an access count

permission, an access time permission, an expiration date permission, an authorization

date permission, a clipboard permission, a print permission, an unlimited access

permission, an application permission, and a system-events permission. Schneck does

teach this feature however, in fig. 3. Therefore it would have been obvious to one of

ordinary skill in the art at the time of the invention to incorporate the features of Schneck

into the system of Saito. Motive to make this combination is found for example, at col. 2

lines 18-27 where the desirability of copyright control systems allowing distributors

control of end user use of copyrighted materials is discussed.

As for claim 68, the combination of Saito and Schneck does not teach the

method of claim 67 further comprising the step of setting a password for access to the

computer executable file. However Official Notice may be taken that the use of such an access password for encrypted files is a step that is old and well known in the art of digital data distribution. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the system of Saito and Schneck. It would have been desirable to do so as this would allow for greater control of end user access to the encrypted content.

Allowable Subject Matter

9.   Claims 3, 6-65, 69-94, 98-128, 131-147, and 149 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

10.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

11.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-

3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's

supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone

number for the organization where this application or proceeding is assigned is: (571)

273-8300.

9-2-06

PEC

Paul Callahan

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER